Amendments to the Claims

Claims 1-20 **(Canceled)**

Claim 21 **(Currently Amended)** The playback terminal of claim ~~20,~~ 42, wherein

the content key obtaining sub-unit, when it is judged that the rights information is required, obtains the license content key used in decrypting of the encrypted content,[[,]] and

the content decryption sub-unit, when it is judged that the rights information is required, decrypts the encrypted content using the license content key.

Claim 22 **(Previously Presented)** The playback terminal of claim 21, wherein

the rights information includes a rights key,

the license content key calculation unit cryptographically calculates the license content key using the rights key of the rights information, and

the content key obtaining sub-unit, when it is judged that the rights information is required, obtains the license content key using the rights key.

Claim 23 **(Canceled)**

Claim 24 **(Currently Amended)** The playback terminal of claim 21, wherein

the portable medium further has ~~stored~~ recorded thereon key obtaining information indicating whether or not the rights information is required for obtaining a key used for decrypting the encrypted content, and

the playback terminal further comprises:

a key obtaining information read unit operable to read the key obtaining information from the portable medium, wherein

the decryption method judgment unit performs the judgment of whether or not the rights information is required for decrypting the encrypted content, based on the key obtaining information.

Claim 25 **(Currently Amended)** The playback terminal of claim ~~20,~~ 42, wherein

the decryption unit, when it is judged that the rights information is ~~necessary~~ required, ~~performs decryption of~~ decrypts the encrypted content only when the communication unit has already acquired the rights information and the rights information indicates that usage of the content is permitted.

Claim 26 **(Canceled)**

Claim 27 **(Currently Amended)** The playback terminal of claim ~~20,~~ 42, wherein

the portable medium further has ~~stored~~ recorded thereon information indicating whether or not the rights information is required for decrypting of the encrypted content, and

the playback terminal further comprises:

an information read unit operable to read the information from the portable medium, wherein

the decryption method judgment unit performs the judgment of whether or not the rights information is required for decrypting the encrypted content, based on the information.

Claim 28 **(Currently Amended)** A content playback method used in a playback terminal for playing back content, the playback terminal having a holding unit that holds device unique information pre-stored in the playback terminal, the device unique information being unique to the playback terminal, the content playback method comprising:

reading encrypted content from a portable medium, the encrypted content being generated by encrypting content using at least medium information including an encrypted medium key, generated by encrypting a medium key with the device unique information, pre-recorded on the portable medium ~~and information pre-stored in the playback terminal~~;

judging whether or not rights information including usage rights for the encrypted content managed by an external license server is required for decrypting the encrypted content;

reading the medium information pre-recorded on the portable medium;

acquiring the rights ~~managed~~ information managed by the external license server when it is judged that the rights ~~managed~~ information is required, the rights ~~managed~~ information

managed by the external license server being a part of information which is required for the decryption of the encrypted content;

decrypting the encrypted medium key, with use of the device unique information, so as to obtain the medium key, and cryptographically calculating a medium content key using the medium key ~~the medium information and the information pre-stored in the playback terminal itself~~;

cryptographically calculating a license content key using the medium content key and the rights ~~managed~~ information acquired from the external license server; and

a decryption step of (a) decrypting the encrypted content using the medium content key, when it is judged that the rights ~~managed~~ information is not required, and (b) decrypting the encrypted content using the license content key, when it is judged that the rights ~~managed~~ information is required, wherein

the decrypting of the encrypted content using the medium content key, when it is judged that the rights information is not required, comprises obtaining the medium content key used in decrypting of the encrypted content and decrypting the encrypted content using the medium content key,

the cryptographically calculating of the medium content key, when it is judged that the rights information is not required, comprises obtaining the medium key by decrypting the encrypted medium key using the device unique information,

the encrypted medium key recorded on the recording medium is generated by encrypting the medium key using device information of valid playback terminals, and

the cryptographically calculating of the medium content key fails to obtain the medium key, when the device unique information of the playback terminal itself is not included in the device information of the valid playback terminals.

Claim 29 **(Cancelled)**

Claim 30 **(Currently Amended)** The content playback method claim ~~29,~~ 28, wherein the decryption step further includes

obtaining, ~~the content key obtaining sub-step includes,~~ when it is judged that the rights information is required, ~~obtaining~~ the license content key used in decrypting of the encrypted content, and

decrypting, ~~the content decryption sub-step includes,~~ when it is judged that the rights information is required, ~~decrypting~~ the encrypted content using the license content key.

Claim 31 **(Currently Amended)** The content playback method of claim 30, wherein

the rights information includes a rights key,

the cryptographically calculating of the license content key comprises cryptographically calculating the license content key using the rights key of the rights information, and

the ~~content key~~ obtaining ~~sub-step includes,~~ of the license content key comprises, when it is judged that the rights information is required, obtaining the license content key using the rights key.

Claim 32 **(Canceled)**

Claim 33 **(Currently Amended)** The content playback method of claim 30, wherein

the portable medium further has ~~stored~~ recorded thereon key obtaining information indicating whether or not the rights information is required for obtaining a key used for decrypting the encrypted content, and

the content playback method further comprises:

reading the key obtaining information from the portable medium, wherein

the judging comprises judging whether or not the rights information is required for decrypting the encrypted content, based on the key obtaining information.

Claim 34 **(Previously Presented)** The content playback method of claim ~~29,~~ 28, wherein

the decrypting of the encrypted content ~~decryption step~~ includes, when it is judged that the rights information is ~~necessary~~ required, decrypting ~~performing decryption of~~ the encrypted content only when the acquiring has already acquired the rights information and the rights information indicates that usage of the content is permitted.

Claim 35 **(Canceled)**

Claim 36 **(Currently Amended)** The content playback method of claim ~~29,~~ 28, wherein

the portable medium further has ~~stored~~ recorded thereon information indicating whether or not the rights information is required for decrypting of the encrypted content, and the content playback method further comprises:

reading the information from the portable medium, wherein

the judging comprises judging whether or not the rights information is required for decrypting the encrypted content, based on the information.

Claims 37 and 38 **(Canceled)**

Claim 39 **(Currently Amended)** The playback terminal of claim ~~20,~~ 42, wherein

the rights information includes information showing permission to play back the content.

Claim 40 **(Currently Amended)** The playback terminal of claim 39, wherein

the portable medium further has recorded thereon information indicating whether or not the rights information is ~~necessary~~ required for decrypting the encrypted content, and

the decryption method judgment unit judges whether or not the rights information is required for decrypting the encrypted content based on the information recorded on the portable medium.

Claim 41 **(Currently Amended)** The content playback method of claim 28, wherein

the managed information managed by the external license server is rights information including usage rights for the content,

the judging comprises judging whether or not the rights information is required, as the information managed by the external license server, for decrypting the encrypted content,

the acquiring comprises acquiring the rights information from the external license server when it is judged that the rights information is required, and

the decryption step comprises (a) decrypting the encrypted content using the medium content key, when it is judged that the rights information is not required, and (b) decrypting the

encrypted content using the license content key, when it is judged that the rights information is required.

Claim 42 **(Currently Amended)** A ~~The~~ playback terminal ~~of claim 26,~~ for playing back content, the playback terminal comprising:

a holding unit operable to hold device unique information pre-stored in the playback terminal, the device unique information being unique to the playback terminal;

a content read unit operable to read encrypted content from a portable medium, the encrypted content being generated by encrypting content using at least medium information including an encrypted medium key, generated by encrypting a medium key with the device unique information, pre-recorded on the portable medium;

a decryption method judgment unit operable to judge whether or not rights information including usage rights for the encrypted content managed by an external license server is required for decrypting the encrypted content;

a medium information read unit operable to read the medium information pre-recorded on the portable medium;

a communication unit operable to acquire the rights information managed by the external license server when it is judged that the rights information is required, the rights information managed by the external license server being a part of information which is required for the decryption of the encrypted content;

a medium content key calculation unit operable to decrypt the encrypted medium key, with use of the device unique information, so as to obtain the medium key, and to cryptographically calculate a medium content key using the medium key;

a license content key calculation unit operable to cryptographically calculate a license content key using the medium content key and the rights information acquired from the external license server; and

a decryption unit operable to (a) decrypt the encrypted content using the medium content key, when it is judged that the rights information is not required, and (b) decrypt the encrypted content using the license content key, when it is judged that the rights information is required, wherein

the decryption unit includes:

a content key obtaining sub-unit operable to, when it is judged that the rights information is not required, obtain the medium content key used in decrypting of the encrypted content; and

a content decryption sub-unit operable to, when it is judged that the rights information is not required, decrypt the encrypted content using the medium content key,

the medium content key calculation unit, when it is judged that the rights information is not required, obtains the medium key by decrypting the encrypted medium key using the device unique information,

the ~~encrypted-state media~~ encrypted medium key recorded on the recording medium is generated by encrypting the ~~media~~ medium key using device information of valid playback terminals, and

the content key obtaining unit fails to obtain the ~~media~~ medium key by decrypting the ~~encrypted-state media~~ encrypted medium key, when the device unique information of the playback terminal itself is not included in the device information of the valid playback terminals.

Claim 43 **(New)** The content playback method of claim 28, wherein

the rights information includes information showing permission to play back the content.

Claim 44 **(New)** The content playback method of claim 43, wherein

the portable medium further has recorded thereon information indicating whether or not the rights information is required for decrypting the encrypted content, and

the judging comprises judging whether or not the rights information is required for decrypting the encrypted content based on the information recorded on the portable medium.